UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P O Box 1450
Alexandria, Virginia 22313-1450
www uspto gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/816,455	03/31/2004	Robert W. Seaton JR.	16222U-014110US	8400

66945 7590 06/23/2008
TOWNSEND AND TOWNSEND CREW LLP
TWO EMBARCADERO CENTER, 8TH FLOOR
SAN FRANCISCO, CA 94111

EXAMINER	
BAYOU, YONAS A	
ART UNIT	PAPER NUMBER
2134	
MAIL DATE	DELIVERY MODE
06/23/2008	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	**Application No.** 10/816,455	**Applicant(s)** SEATON ET AL.	
	Examiner YONAS BAYOU	**Art Unit** 2134	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 April 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-8 and 10-34* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-8 and 10-34* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *03/31/2004* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)

2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)

3) ☐ Information Disclosure Statement(s) (PTO/SB/08)
Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. _____ .

5) ☐ Notice of Informal Patent Application

6) ☐ Other: _____.

DETAILED ACTION

1. This office action is in response to applicant's response filed on 04/22/2008.

2. Claims 1-8 and 10-34 are pending.

3. Claim 9 is cancelled.

4. Applicant's arguments have been fully considered but they are not persuasive.

5. When responding to the Office action, Applicant is advised to clearly point out the patentable novelty the claims present in view of the state of the art disclosed by the reference(s) cited or the objection made. A showing of how the amendments avoid such references or objections must also be present. See 37 C.F.R. 1.111(c).

Response to Arguments

1. Applicant, on page 10, of the remarks, argues in the method of claim 1, "Hodgson does not teach an Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN), and configured to request a passcode corresponding to the PAN; and

a front end Hardware Security Module (HSM) coupled to the ACS, and configured to receive the passcode in an encrypted format and generate an encrypted passcode using a local encryption key."

Examiner respectfully disagrees and asserts that Hodgson discloses that refer to FIGS. 2A through 2C. At step 200, the process is started. At step 205, the consumer using consumer PC 12 browses a merchant web site on the Internet merchant server 20 over the Internet 18. At step 207, the consumer using consumer PC 12 selects one or more items from the merchants+ Internet web site 20. When the consumer is finished shopping, he or she initiates a secure payment transaction at step 208 according to the present invention, by "clicking" on a button on the merchant's checkout page that triggers the STS-MF 22. At step 209, an HTML payment page is built at the merchant server 20 by the STS-MF 22 and sent to the consumer PC 12. A browser script contained in the HTML payment pages will present a series of prompts to the consumer at the consumer PC 12, as shown in FIGS. 5-10. These screens will walk the consumer through the process of building a secure message as described in detail herein. As part of the process of building the HTML page and script, a Message Authentication Code (MAC) is generated, encrypted and hidden in the HTML payment page shown in FIG. 5. This will be used later to verify that the transaction amount was not altered after the HTML page and script is sent from the merchant web site 20. Other encryption or hash routines might be used for the purpose of preventing subsequent alteration **[see, para. 90 and fig. 2A]**.

And the FP Block is decrypted at the STMS using decryption algorithm(s) matching that used by the software at the consumer's Internet access device. The encrypted PIN block within this data will be translated (deencrypted and re-encrypted) by a Hardware Security Module (HSM) **[see, para. 30]**.

2. Examiner, however, in light of the above submission maintains the previous rejections while considering the amendments to the claims as follows:

Claim Rejections - 35 USC § 102

1. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

2. Claims 1-32 are rejected under 35 U.S.C. 102(b) as being anticipated by Hodgson et al., Pub. No. US 2002/0123972 A1 (hereinafter Hodgson).

Referring to claims 1, 6 and 11, Hodgson teaches a secure passcode authentication system, the system comprising:

an Access Control Server (ACS) configured to receive a request for passcode authentication of a Primary Account Number (PAN), and configured to request a passcode corresponding to the PAN **[paragraph 90 and figs. 2A;** step 210, entering their data and sending to the STMS corresponding to passcode for passcode authentication];

a front end Hardware Security Module (HSM) coupled to the ACS, and configured to receive the passcode and generate an encrypted passcode using a local encryption key **[paragraph 30]**; and

a back end HSM configured to receive the encrypted passcode from the front end HSM and further configured to recover a clear form of the passcode, generate a back end encrypted passcode, and communicate the back end encrypted passcode to an authentication network **[paragraph 0057, paragraph 0061, lines 11-14 and figs. 1 and 1A**, STMS 30 handles all the payment transaction request over the internet 18].

Referring to claim 2, Hodgson teaches a secure passcode authentication system, wherein the request for passcode authentication comprises a request for a Personal Identification Number (PIN) authentication **[paragraph 0005, lines 24-28].**

Referring to claim 3, Hodgson teaches a secure passcode authentication system, wherein the ACS is further configured to receive an authentication message from the authentication network **[paragraph 0090, lines 6-20 and figs. 2A-2C].**

Referring to claim 4, Hodgson teaches a secure passcode authentication system, wherein the ACS is further configured to generate a unique transaction identification and include the unique transaction identification as a hidden field in the request for the passcode **[paragraph 0098, lines 5-7 and fig. 2C].**

Referring to claim 5, Hodgson teaches a secure passcode authentication system, wherein the front end HSM is configured to generate a hash value based in part on the unique transaction identification, and wherein the ACS is configured to include the hash value as an additional hidden field in the request for the passcode **[paragraph 0027 and paragraph 0154].**

Referring to claims 7 and 25, Hodgson teaches a secure passcode authentication system, wherein the front end HSM comprises a software HSM **[paragraph 0023]**.

Referring to claim 8, Hodgson teaches a secure passcode authentication system, wherein the front end HSM comprises a hardware HSM **[paragraph 0023].**

Referring to claims 10, 22-24 and 30, Hodgson teaches a secure passcode authentication system, wherein the first encrypted format comprises a Secure Sockets Layer (SSL) encrypted format **[paragraph 0076].**

Referring to claim 12, Hodgson teaches a secure passcode authentication system, wherein the front end HSM is configured to receive a cardholder encrypted passcode from a cardholder device **[paragraph 0019,** pin/pad is corresponding to a cardholder device].

Referring to claim 13, Hodgson teaches a secure passcode authentication system, wherein the back end HSM is configured to generate the back end encrypted passcode by generating a PINBLOCK using the clear form of the passcode and encrypting the PINBLOCK using an Acquirer Working Key (AWK) **[paragraph 0073,** DES or ATM is corresponding to AWK].

Referring to claim 14, Hodgson teaches a secure passcode authentication system, wherein the authentication network comprises an Internet Payment Gateway Server (IPGS) **[paragraph 0066, paragraph 0099, lines 18-20,** IPGS corresponds to STS-MF 22 which is inside of the merchant server 20].

Referring to claim 15, Hodgson teaches a secure passcode authentication system, wherein the authentication network further comprises an issuer server coupled to the IPGS **[paragraph 0060, lines 7-8].**

Referring to claims 16, 20, 31 and 32, Hodgson teaches a secure passcode authentication system, the system comprising:

an Access Control Server (ACS) configured to receive a request for Personal Identification Number (PIN) authentication of a Primary Account Number (PAN), and configured to generate a request for a PIN corresponding to the PAN **[paragraph 0062]**, the request for the PIN including hidden fields comprising a unique transaction identifier and a hash value **[paragraph 0027 and paragraph 0154].**

a front end Hardware Security Module (HSM) coupled to the ACS **[paragraph 0154]**, and configured to generate the hash value based in part on the unique transaction identifier **[paragraph 0027 and paragraph 0154]**, and further configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN **[paragraph 0030]**, and generate a local encrypted PIN using a local encryption key **[paragraph 0154]**; and

a back end HSM configured to receive the local encrypted PIN from the front end HSM and further configured to recover a clear form of the PIN from the local encrypted PIN **[paragraph 0057, paragraph 0061, lines 11-14 and fig. 1A]**, generate an Acquirer Working Key (AWK) encrypted PIN, and communicate the AWK encrypted PIN to an authentication network **[paragraph 0073].**

Referring to claim 17, Hodgson teaches a secure passcode authentication system, wherein the front end HSM generates the local encrypted key using a triple DES algorithm **[paragraph 0154].**

Referring to claims 18 and 21, Hodgson teaches a secure passcode authentication system, the system comprising:

an Access Control Server (ACS) configured to receive a request for Personal Identification Number (PIN) authentication of a Primary Account Number (PAN), and configured to generate a request for a PIN corresponding to the PAN, the request for the PIN including an instruction to provide the PIN to a destination address **[paragraph**

0062 and paragraph 0087, STMS 30 sends a follow up email to the email addressed used to register the PIN/PAD 16]; and

a front end Hardware Security Module (HSM) having said destination address and coupled to the ACS **[paragraph 0154 and paragraph 0087]**, and configured to receive an encrypted PIN, decrypt the PIN to recover a clear form of the PIN **[paragraph 0030]**, and generate an Acquirer Working Key (AWK) encrypted PIN using an AWK encryption key, and configured to communicate the AWK encrypted PIN to an authentication network **[paragraph 0073].**

Referring to claims 19, 27 and 28, Hodgson teaches a method for providing secure passcode authentication, the method comprising:

requesting a Personal Identification Number (PIN) corresponding to a Primary Account Number (PAN) **[paragraph 0062]**;

receiving the PIN in response to the request **[paragraph 0062]**;

generating a PINBLOCK based in part on the PIN **[paragraph 0073]**;

encrypting the PINBLOCK using a local key in a front end Hardware Security Module (HSM) to generate a local key encrypted PINBLOCK **[paragraph 0073]**;

decrypting the local key encrypted PINBLOCK with a back end HSM **[paragraph 0030]**;

generating a back end encrypted PIN with the back end HSM **[paragraph 0057]**;

communicating the back end encrypted PIN to an authentication network **[paragraph 0005, lines 19-22]**; and receiving an authentication response from the authentication network **[paragraph 0090, lines 6-20 and figs. 2A-2C].**

Referring to claim 26, Hodgson teaches a method for providing secure passcode authentication, wherein encrypting the PINBLOCK comprises encrypting the PINBLOCK using a triple DES encryption algorithm **[paragraph 0026].**

Referring to claim 29, Hodgson teaches a method for providing secure passcode authentication, wherein the front end HSM comprises the back end HSM **[paragraph 0057].**

Conclusion

THIS ACTION IS MADE FINAL. Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONAS BAYOU whose telephone number is (571)272-7610. The examiner can normally be reached on m-f,7:30-5:00.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kambiz Zand can be reached on 571-272-3811. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Yonas Bayou/

Examiner, Art Unit 2134

06/18/2008

/Kambiz Zand/

Supervisory Patent Examiner, Art Unit 2134